MCSE Guide to Designing Microsoft Windows 2000 Security

Conan Kezema, Stanley Reimer

COURSE TECHNOLOGY
THOMSON LEARNING

Australia • Canada • Mexico • Singapore • Spain • United Kingdom • United States

MCSE Guide to Designing Microsoft Windows 2000 Security

by Stanley Reimer and Conan Kezema

Product Manager:
Charles Blum

Production Editor:
Christine Spillett

Developmental Editor:
Moirag Haddad

Quality Assurance Manager:
John Bosco

Quality Assurance Tester:
Nicole Ashton

Associate Product Manager:
Tim Gleeson

Editorial Assistant:
Nick Lombardi

Marketing Manager:
Toby Shelton

Text Designer:
GEX Publishing Services

Compositor:
GEX Publishing Services

Cover Design:
Joseph Lee, Black Fish Design

Printed in Canada

1 2 3 4 5 6 7 8 9 WC 06 05 04 03 02

For more information, contact Course Technology, 25 Thomson Place, Boston, Massachusetts, 02210.

Or find us on the World Wide Web at: www.course.com

ISBN 0-619-01688-4

BRIEF

Contents

TABLE OF

Contents

Preface

Welcome to the *MCSE Guide to Designing Microsoft Windows 2000 Security*! This book provides in-depth coverage of the knowledge and skills required to pass Microsoft certification exam 70-220: *Designing Security for a Microsoft Windows 2000 Network*. This course of study prepares a network professional to have the ability to design network security solutions. These solutions include analysing business requirements, identifying security needs, and applying the security recommendations to assist in the control and monitoring of network and service resources.

The Intended Audience

The goal of this book is to teach strategies for security design to individuals who desire to learn about that topic for practical purposes, as well as those who wish to pass Microsoft exam, #70-220. This book provides the content for all the skills measured on that exam, but also provides related information that is not directly tested.

Chapter 1, "Identifying Security Risks" provides an overview of internal and external security risks and identifies general principals for managing those risks. Chapter 2 "Corporate Components to Security Planning" emphasizes the importance of collecting information before designing a security plan. It shows how to identify existing and planned business models, existing company processes, organizational structures, company strategies, and IT management structure. Chapter 3, "Securing Resources on Windows 2000 Servers" outlines how to control access to the various resources available on the network. Various authentication protocols are described and information is provided about how to plan and configure an audit policy.

Chapter 4, "Designing Active Directory for Security" identifies and explains various Active Directory components and how to design a secure Organizational Unit structure. This chapter teaches how to design and implement Account Policies, and how to delegate control of administrative tasks. It then describes how Group Policy can be used to configure and implement an effective security plan. Chapter 5, "Implementing a Public Key Infrastructure", focuses on the concepts of Public Key Infrastructure and how it can be used to enhance security in Windows 2000.

Chapter 6 "Securing Network Services" describes how to implement Windows 2000 DNS and DHCP, and how to plan secure implementations of Remote Installation Services and SNMP, as well as secure access for non-Microsoft clients. The concept of securing servers

using Security templates is also discussed. Chapter 7 "Securing Network Communications" describes how to plan a secure network communication implementation using Server Block Signing. This chapter also teaches how to plan and implement secure network transmission by implementing IP security (IPSec).

Chapter 8 "Securing Access for Remote Access Users" looks at the issues involved in implementing access for dial-up clients and VPN clients. It also discusses enhanced security for Windows 2000 remote access, and how to plan and use remote access policies. RADIUS is also introduced to assist in situations where multiple RRAS servers are implemented.

Chapter 9 "Securing Access Between Corporate Locations" looks at the security risks that exist for information passing between corporate locations. This chapter also outlines how to implement and secure Windows 2000 when it is configured as a router, or as a VPN server. It then describes secure network access for partner organizations.

Chapter 10 "Designing Secure Access to the Internet" covers how to secure an internal corporate network by implementing various security services, such as NAT, firewalls, and Demilitarized Zones. It also describes secure user access through the use of proxy services, such as MS Proxy 2.0 and Internet Security and Acceleration Server 2000. In addition, this chapter teaches how to design and implement a corporate Internet usage policy.

FEATURES

To ensure a successful learning experience, this book includes the following pedagogical features:

- **Chapter Objectives:** Each chapter in this book begins with a detailed list of the concepts to be mastered within that chapter. This list provides you with a quick reference to the contents of that chapter, as well as a useful study aid.
- **Illustrations and Tables:** Numerous illustrations of server screens and components aid you in the visualization of common setup steps, theories, and concepts. In addition, many tables provide details and comparisons of both practical and theoretical information and can be used for a quick review of topics.
- **End-of-Chapter Material:** The end of each chapter includes the following features to reinforce the material covered in the chapter:
  - **Summary.** A bulleted list is provided which gives a brief but complete summary of the chapter
  - **Review Questions.** A list of review questions tests your knowledge of the most important concepts covered in the chapter
  - **Key Terms List.** A list of all new terms and their definitions

- **Hands-on Projects.** Hands-on projects help you to apply the knowledge gained in the chapter
- **Case Study Projects.** Case study projects take you through real world scenarios

■ **On the CD-ROM.** On the CD-ROM you will find **CoursePrep** exam preparation software, which provides 50 sample MCSE exam questions mirroring the look and feel of the MCSE exams

TEXT AND GRAPHIC CONVENTIONS

Wherever appropriate, additional information and exercises have been added to this book to help you better understand what is being discussed in the chapter. Icons throughout the text alert you to additional materials. The icons used in this textbook are as follows:

Tips are included from the author's experience and provide extra information on resources related to network design.

The Note icon is used to present additional helpful material related to the subject being described.

Each Hands-on Project in this book is preceded by the Hands-on icon and a description of the exercise that follows.

Case project icons mark the case project. These are more involved, scenario-based assignments. In this extensive case example, you are asked to implement independently what you have learned.

INSTRUCTOR'S MATERIALS

The following supplemental materials are available when this book is used in a classroom setting. All of the supplements available with this book are provided to the instructor on a single CD-ROM.

Electronic Instructor's Manual. The Instructor's Manual that accompanies this textbook includes:

- Additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.
- Solutions to all end-of-chapter materials, including the Review Questions, Hands-on Projects and Case Projects.

ExamView. This textbook is accompanied by ExamView, a powerful testing software package that allows instructors to create and administer printed, computer (LAN-based), and Internet exams. ExamView includes hundreds of questions that correspond to the topics covered in this text, enabling students to generate detailed study guides that include page references for further review. The computer-based and Internet testing components allow students to take exams at their computers, and also save the instructor time by grading each exam automatically.

PowerPoint presentations. This book comes with Microsoft PowerPoint slides for each chapter. These are included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors, please feel at liberty to add your own slides for additional topics you introduce to the class.

Read This Before You Begin

To the User

This book was written with the network professional in mind. It provides an excellent preparation for the Microsoft exam 70-220, and also for the real-life tasks involved in designing network security for today's networks, which must support an ever-increasing variety of applications. To fully benefit from the content and the projects presented here, you will need access to a classroom lab containing computers configured as follows:

- Windows 2000 Advanced Server installed with the default settings. Name each computer server1, server2, etc. It is recommended to have 2 network cards in each computer.
- Run dcpromo.exe to upgrade the server to a domain controller. Install DNS when prompted. Use Lonestar.com as the domain name. Change the zone type to Standard Primary.
- For the Domain Users group, add the right to log on locally to the domain controllers security policy.

Visit Our World Wide Web Site

Additional materials designed especially for you might be available for your course on the World Wide Web. Go to *www.course.com*. Search for this book title periodically on the Course Technology Web site for more details.

TO THE INSTRUCTOR

The Hand-on projects should meet the hardware requirements listed below:

Hardware Component	Windows 2000 Advanced Server
CPU	Pentium II 200 or higher
Memory	128 MB RAM
Disk Space	1 GB minimum for partition containing system files
Drives	CD-ROM Floppy Disk
Networking	TCP/IP 2 Network adapters Card 1 – 131.107.1.1: Label: Internal Card 2 – 131.107.2.1: Label: External Install DHCP but do not activate the scope (scope: 131.107.1.5 – 131.107.1.10)
	A connection to the Internet via some sort of NAT or Proxy server is assumed.

1. Install Windows 2000 Advanced server. Name the computer **Server1**.
2. Run dcpromo.exe to upgrade the server to a domain controller. Install DNS when prompted. Use Lonestar.com as the domain name. Change the zone type to Standard Primary.
3. For the Domain Users group, add the right to log on locally to the domain controllers security policy.
4. Detailed setup instructions for the labs are contained in the Instructor's Manual.